Deteksi, Monitoring Dan Pencegahan Insider Threat : As A Survey

Muhamad Firmansyah[1], Yurry Matufira[2], Beny Nugraha[3]
Universitas Mercu Buana
muhfirmansyah@gmail.com[1], *yurry.umb@gmail.com[2], benynugraha@mercubuana.ac.id[3]*

Abstract - many organizations using networks such as the Internet in data management. With a network of course the threat continues to threaten the confidentiality, integrity and availability of the system. Many organizations do this prevention, but they usually focus on the threat from the outside. The threat from within is more easily abuse the access authority often escape the focus of prevention.
Has been a lot of research that explores the problems of insider threat. The approach taken out of the habit theory proposed by Moyano, Bayesian Network models and preliminary model of the End User Computing (EUC).
This paper defines the threat from within (Insider Threat) with techniques of detection and prevention, and then do the mapping for the management of the system against the insider threat.
Keywords: insider threats, detection, monitoring, sociology, management system

Abstrak – Organisasi banyak menggunakan jaringan seperti internet dalam pengelolaan data. Dengan jaringan tentu saja ancaman senantiasa mengancam *confidentiality*, *integrity* dan *availability* system. Banyak organisasi melakukan pencegahan ini, namun biasanya fokus mereka pada ancaman dari luar. Adapun ancaman dari dalam yang lebih mudah menyalahgunakan otoritas akses sering luput dari fokus pencegahannya.

Telah banyak penelitian yang mengetengahkan permasalahan *insider threat*. Pendekatan diambil dari teori kebiasaan yang diajukan oleh Moyano, model Bayesian Network dan model preliminary pada End User Computing (EUC).

Tulisan ini mendefinisikan ancaman dari dalam (*Insider threat*) dengan teknik-teknik pendeteksian dan pencegahannya dan kemudian melakukan pemetaan untuk pengelolaan manajemen sistem terhadap *insider threat*.
Kata kunci: insider threat, detection, monitoring, sociology, system management

1. Latar Belakang

Organisasi membutuhkan jaringan seperti internet untuk mempermudah alur pengelolaan informasi di dalamnya. Dengan banyaknya pengguna internet mengakibatkan organisasi harus memilah data dan informasi yang dapat diakses public dan yang tidak. Dari sini keamanan jaringan adalah fokus penting yang dipersiapkan dengan baik oleh organisasi.

Banyak organisasi yang memfokuskan diri pada keamanan dari pihak eksternal, padahal keamanan Insider Threat adalah ancaman yang terselubung dan sangat mematikan. Selain itu, kerugian yang dihasilkan oleh insider threat jauh lebih besar dibandingkan oleh penyerang dari luar.

Insider Threat yang dapat menjadi ancaman adalah pegawai, mantan pegawai ataupun pihak ketiga yang memiliki wewenang akses baik pada jaringan, informasi maupun data pada organisasi (Nurse et al., 2014),

Memilah mana Insider Threat yang menjadi ancaman ataupun yang tidak sangatlah sulit. Hanya saja, pembahasan mengenai insider threat perlu dilihat dari aspek teknis dan sosiologis. Insider Threat ternyata memang dirasakan sekali dimana menurut (Anning & IBM, 2015), US Bureau of Justice Statistics melaporkan 40 % insiden dan 93 persen cyber theft justru dilakukan oleh Insider Threat termasuk didalamnya adalah intellectual property theft.

Kami mengajukan taksonomi insider threat dilihat dari sisi sosiologis dan teknis untuk pemetaan lingkup deteksi dan pencegahan pada tulisan ini. Tulisan ini merupakan survey beberapa pendekatan yang telah diajukan dengan melihat aspek psikososial dan teknis untuk mengidentifikasi maupun mencegah terjadinya ancaman internal. Aspek sosiologis mengadopsi pendekatan (Kammuller & Probst, 2015) yang memadukan antara aspek sosiologi dan pendekatan formal computer. Untuk aspek teknis, kami mempelajari berbagai teknik yang diajukan oleh banyak peneliti seperti (Bowen, Ben Salem, Hershkop, Keromytis, & Stolfo, 2009) melalui model monitoring berbasis sensor. Selain itu kami juga mempelajari pendekatan menggunakan

software honeypots yang dapat digunakan untuk menangkap insider threat seperti yang diajukan oleh (Spitzner, Technologies, & Inc, 2003).

2. Karakteristik Insider Threat

Setiap orang dalam suatu organisasi yang diberi otoritas untuk melakukan akses jaringan maupun data organisasi dan melakukan tindakan jahat dengan penyalahgunaan otoritas disebut *Insider Threat*. *Insider Threat* ini bisa merupakan pegawai, mantan pegawai, kontraktor, maupun pihak ketiga yang dipercaya organisasi untuk masuk ke dalam sistem. *Insider Threat* yang dapat menjadi ancaman dikategorikan sebagai berikut :

a. *Malicious Insider threat*

Insider Threat ini membawa *malicious code* yang menyalahgunakan wewenang aksesnya untuk mengganggu *integrity, confidentiality* maupun *availability* yang dimiliki oleh sistem. *Insider Threat* ini melakukan ancaman tersebut untuk mencapai tujuan-tujuan penyalahgunaan kebijakan yang ditetapkan oleh organisasi.

b. *Accidental Insider threat*

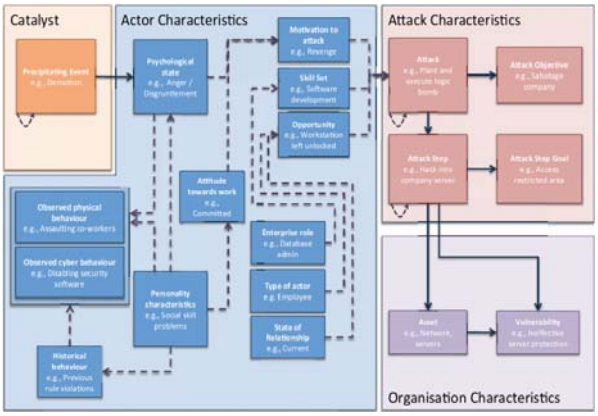
Insider Threat tanpa malicious code tapi dengan ataupun tanpa kesengajaan melakukan gangguan terhadap integrity, confidentiality ataupun availability sistem. Hal ini terjadi karena buruknya sistem dalam penanganan maupun pencegahan terhadap insider threat.

Dalam system computer, insider threat sangat erat kaitannya dengan pengaksesan file atau pengeksekusian program yang mana hal ini dapat dipantau melalui log yang tak akan lepas dengan catatan user pengakses ataupun pengeksekusinya (Nguyen, Reiher, & Kuenning, 2003).

Pemantauan dapat dilakukan dengan model *user oriented monitoring* ataupun *process oriented monitoring.* Pada *user oriented monitoring,* adalah suatu kewajaran jika X yang merupakan seorang programmer selalu mengakses direktori project, maka selain itu dianggap bukan suatu kewajaran. Sementara pada *process oriented monitoring*, merupakan catatan tersendiri jika ditemukan bahwa seorang user mengakses ataupun mengeksekusi berkas dengan cara yang tidak biasa.

User sendiri terbagi menjadi 2 jenis yang berbeda jika dilihat dari sisi alamiahya. User berupa manusia yang bersifat lebih interaktif, kompleks dan dinamis. Jenis yang lain adalah user berupa system yang hanya melakukan tugas tertentu saja.

Dalam hal mengenal karakteristik *Insider Threat* tersebut Nurse et, al mengemukakan framework sistem seperti pada gambar 1.



Gambar 1. Framework karakterisasi insider threat

Dikemukakan oleh (Nurse et al., 2014), bahwa untuk mengenal karakteristik *insider threat* perlu memerankan sosiologi dalam menimbang seseorang berpotensi menjadi insider threat atau tidak. Hal-hal psikologis, melalui sejarah penggunaan teknologi seperti pengiriman surel, penggunaan workstation dan motivasi penyerangan adalah langkah efektif untuk memprediksi *insider* tersebut melakukan penyerangan terhadap *asset* dan *vulnerability* sistem dalam organisasi.

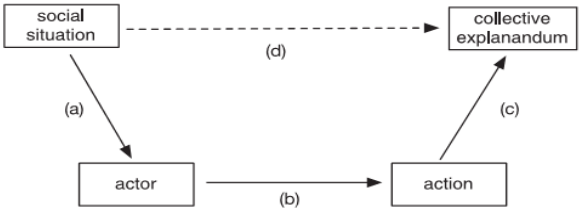
Dalam tulisan lain, (Chinchani, Iyer, Ngo, & Upadhyaya, 2005) insider attack melakukan fase pengintaian yang sangat singkat waktunya guna mencari kesempatan melakukan perusakan pada system baik berupa DoS, pencurian informasi atau hal jahat lainnya. Dalam melancarkan serangannya, insider akan menabrak pihak insider lain atau melakukan kompromi terlebih dahulu,

3. Deteksi dan Pencegahan *Insider Threat*

Secara kebiasaan ada 3 aktor yang berperan dalam melakukan serangan yaitu petugas informasi, petugas keamanan dan penyerang dalam (Martinez-Moyano, Rich, Conrad, Andersen, & Stewart, 2008). Petugas informasi menggunakan tugas rutin dan transaksi-transaksi yang tersedia dalam sistem guna menghasilkan keuntungan organisasi, sementara itu petugas keamanan berperan dalam mengembangkan keamanan berupa strategi perlindungan sistem. Penyerang dari dalam akan memperhitungkan waktu yang tepat dalam melakukan serangan setelah mendapatkan akses karena ada celah dimana petugas informasi tidak mengikuti ketentuan keamanan yang ditetapkan oleh petugas keamanan. Oleh karena itu, langkah terbaik untuk melakukan pemilahan apakah ada penyerang dari dalam adalah dengan

menyediakan fitur interaksi pada sistem dalam suatu organisasi.

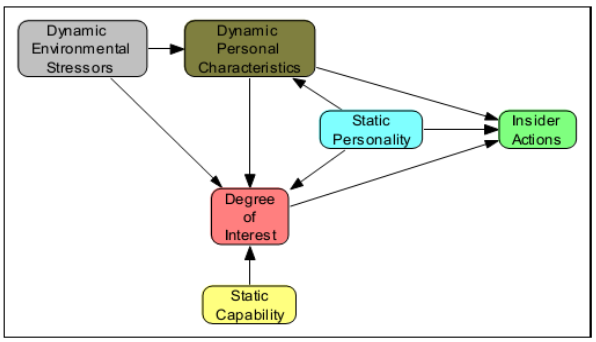
Dalam hal melakukan verifikasi, perlunya memadukan aspek sosiologis dan metode formal computer (Kammuller & Probst, 2015). Mereka mengintegrasikan organisasi, kebijakan dan aktor pada sistem cyberhuman. Tahapan penjelasan sosiologis terbagi menjadi 3 tahap yaitu (a) penterjemahan situasi, (b) diterjemahkan oleh aktor menjadi sebuah aksi, (c) efek aksi yang dilakukan oleh aktor. Hal ini dapat dilihat pada gambar 2.



Gambar 2. Penjelasan Sosiologis "Grundmodell"

Pada paper ini, penjelasan sosiologis diterapkan menggunakan *Higher Order Logic* (HOL) dimana *Object Logic* memungkinkan penerjemahan file yang mengandung *object logic* berdasarkan penjelasan sosial.

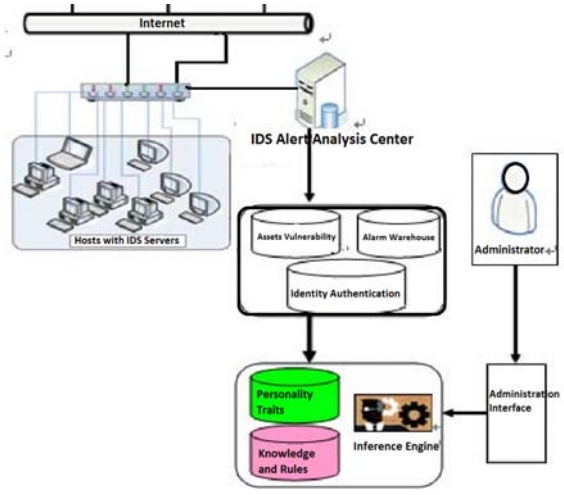
Selain pendekatan tersebut, dapat juga menggunakan model Bayesian Network (Axelrad & Sticha, 2013) dengan melakukan pengembangan daftar yang berpotensi terintegrasi dengan *insider attacker.* Daftar tersebut selanjutnya diberikan peringkat dan dinilai menggunakan model Bayesian Network. Model Bayesian Network melakukan prediksi dengan membandingkan daftar dan algoritma perbandingannya. Hal ini dapat dilihat pada gambar 3.



Gambar 3. Konsep Model Bayesian Network

Kekhawatiran lain pada sisi insider adalah kemampuannya menggunakan sistem IT sehinga terjadi kesalahan penggunaan, dimana hal ini menjadi celah bagi penyerang luar untuk dimanfaatkan menjadi serangan ke dalam sistem (Magklaras & Furnell, 2005). Paper [6] menggambarkan pendekatan prediksi *insider threat* akibat kesalahan penggunaan dalam sistem IT pada model *End User Computing (EUC) sophistication*. Pada model ini mengangkat 3 hal yang menjadi pokok perhatian yaitu seberapa luas pengguna memahami sistem IT, seberapa dalam pengguna mampu mengoperasikan sistem IT dan seberapa mahir pengguna menggunakan sistem IT. Untuk itu, maka perlunya proses otomatisasi untuk mengurangi tingkat kesalahan pada pengguna agar memperkecil kemungkinan celah pemanfaatan kesalahan penggunaan oleh penyerang eksternal.

Modul yang digunakan untuk mengevaluasi adanya *insider threat* harus mengintegrasikan dan memanfaatkan jaringan berbasis sensor (Wang & Yang, 2014). Hal ini memfokuskan kepada hal-hal yaitu log aktivitas karyawan, akun yang sudah mati, akses unauthorized pada perangkat, akses berlebihan, frekuensi waktu yang tidak normal dan karakter personal. Selain hal tersebut, perlu juga mempertimbangkan bukti jika ada serangan guna memberi kemampuan pelacakan dimana keseluruhan konsep tersebut dijabarkan dalam model sistem dinamis. (Wang & Yang, 2014) mengemukakan model dinamis yang dapat dilihat pada gambar 4.

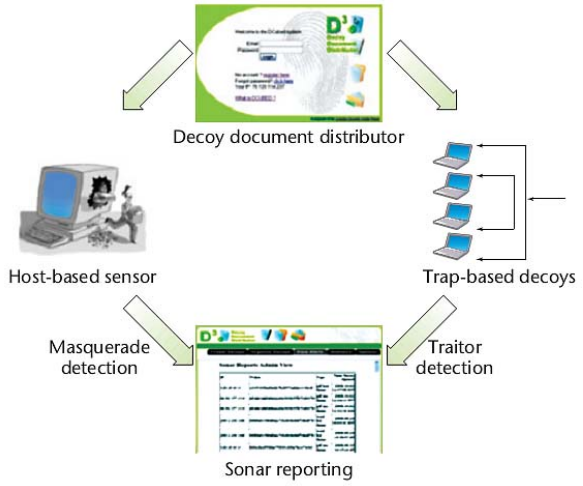


Gambar 4. Konsep Model Sistem Dinamis

Untuk melakukan pencegahan terhadap *insider threat* sangatlah sulit, karena pihak yang menjadi ancaman adalah internal. Hal termungkin dalam mengurangi resiko adalah melalui manajemen sistem dengan sebaik-baiknya dengan

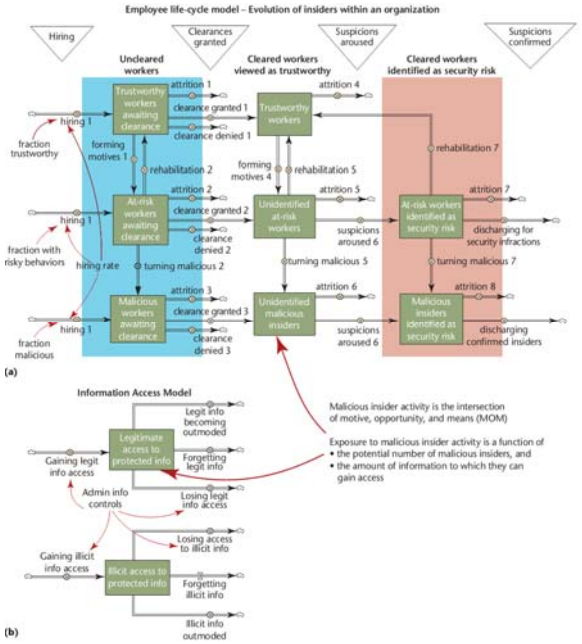
memperhatikan Motive, Opportunity dan Mean (MOM) (Durán, Conrad, Conrad, Duggan, & Held, 2009), Bagi insider threat, motif adalah hal yang mendorongnya menjadi ancaman melalui aktivitas jahat seperti uang, balas dendam, ketidakpuasan maupun harga diri. (Cert & Cert, 2008),

Pendekatan alternatif adalah mengurangi resiko akibat insider threat melalui teknik deteksi dan monitoring. Salah satunya adalah dengan mengembangkan monitor berbasis sensor (Bowen, Ben Salem, Hershkop, Keromytis, & Stolfo, 2009), Mereka mengajukan desain yang terdiri dari 3 komponen utama yaitu dokumen umpan, komponen jaringan dan sensor berbasis host. Desain ini menerapkan dokumen umpan yang terhubung pada jaringan termonitor dan sensor yang secara kolektif mengumpulkan data audit guna mengidentifikasi pengguna spesifik. Rancangan tersebut dapat dilihat pada gambar 5.



Gambar 5. Desain Host Based Network Sensor

Pegawai merupakan elemen kunci yang perlu dimenej sedemikian rupa untuk mengurangi dampak insider threat (Durán et al., 2009), Untuk itu diajukan model employee life cycle yang mencoba memberi pemahaman kepada pegawai untuk berinteraksi menuju sistem kepegawaian yang mengandung prosedur-prosedur yang mampu mengarahkan kemudahan investigasi saat terjadinya gangguan oleh insider threat. Pendekatan yang diajukan bersifat system based yang mengedepankan business process untuk mendapatk legitimasi pegawai dalam mndapatkan akses pada system. Model ini dipresentasikan melalui gambar 6.

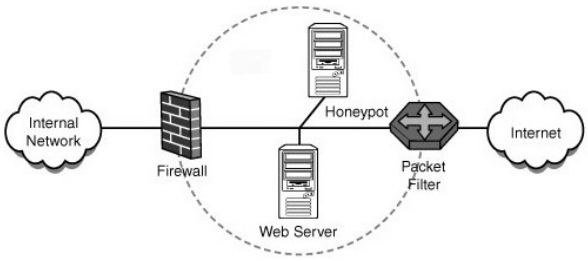


Gambar 6. Model Employee Life Cycle

Dalam hal teknologi, beberapa pendekatan dilakukan untuk mengidentifikasi *insider threat*. Melalui *anomaly graph-based* (Eberle, Holder, & Graves, 2011), saat penggalian data digambarkan ke dalam sebuah grafik yang memperlihatkan anomali dari aktivitas-akitivitas yang dianggap normal. Pendekatan tersebut lahir melalui prinsip pencarian deviasi rata-rata pada penghapusan tepi data pada *minimum data length* (*MDL*) digabung dengan pendekatan probabilitas.

Ada juga pendekatan melalui pembangunan sistem otonom guna memaksa aktivitas dalam jaringan tunduk pada security policy yang dibangunnya melalui Autonomic Violation Prevention System (AVPS) (Sibai & Menasce, 2011), Melalui sistem tersebut, segala bentuk *request* yang merusak akan drop, dipentalkan dan digugurkan sebelum mencapai host.

Selain hal-hal tersebut di atas, honeypots juga digunakan untuk mendeteksi serta menangkal adanya insider threat yang berupaya melakukan aktivitas-aktivitas jahat seperti pencurian kartu kredit, pencurian data, ataupun aktivitas jahat lainnya (Spitzner, Technologies, & Inc, 2003). Arsitektur system menggunakan honeypots dapat dilihat pada gambar 7.



Gambar 7. Penggunaan honeypots dalam sistem

4. Pengelolaan Insider Threat

Dalam survey ini, penulis melakukan pemetaan dalam manajemen penanggulangan *insider threat*. Masing-masing elemen dilakukan pendekatan secara sosiologi dan teknologi seperti yang terlihat pada Tabel 1.

Tabel 1. Pemetaan Manajemen *Insider Threats*

Element	Approaches	
	Sociology	Technology
Employee	Motivation	Force into system
External	Anomaly	Catch
Environment	Policy	Verification

Telah disinggung sebelumnya bahwa pihak internal yang menjadi aktor adalah pegawai baik mantan maupun sedang berstatus pegawai, pihak ketiga maupun kontraktor yang kami kategorikan sebagai employee. Sementara pihak eksternal adalah pihak yang ingin mengambil keuntungan dari system yang ada baik berupa malicious code ataupun kelalaian dari pihak employee. Environment adalah sistem yang dijalankan dalam organisasi ataupun perusahaan.

Secara sosiologi, pendekatan yang dilakukan hampir berbaur dengan teknologi, tetapi pada pihak internal dan environment merupakan wewenang penuh organisasi maupun perusahaan untuk mengelolanya baik berupa training pegawai terhadap sistem yang digunakan, pemberian pemahaman pada employee, penentuan aturan main ataupun penyusunan kebijakan dalam rangka pengamanan system.

Secara teknologi, employee dipaksa untuk menjalankan sistem untuk beraktivitas. Sedangkan eksternal ditangkap dan dipentalkan agar tidak mampu mencapai host dalam lingkungan yang penuh dengan verification.

5. Penutup

Melakukan pencegahan terhadap insider threat adalah hal yang sangat sulit, sehingga pendekatan-pendekatan yang dilakukan adalah melalui sosiologi dan teknologi yang mengarah kepada pemahaman akan stabilisasi system jaringan.

Namun demikian, perlu perhatian lebih terhadap insider threat yang secara potensial lebih membawa kerugian kepada organisasi dibandingkan penyerang eksternal. Pendekatan-pendekatan lain dibutuhkan guna mengurangi lebih banyak lagi potensi ancaman ini, mengingat insider threat adalah pihak dalam yang lebih mengetahui celah keamanan di dalam system dimana mereka ada di dalamnya.

6. Pustaka

[1] Anning, S., & IBM. (2015), *The Insider Threat*, tersedia di http://www.fbi.gov/about-us/investigate/counterintelligence/insider_threat_brochure.

[2] Axelrad, E. T., & Sticha, P. J. (2013), *A Bayesian Network Model for Predicting Insider Threats*, artikel jurnal pada Security and Privacy Workshops, 82–89.

[3] Bowen, B. M., Ben Salem, M., Hershkop, S., Keromytis, A. D., & Stolfo, S. J. (2009), *Designing host and network sensors to mitigate the insider threat*, artikel jurnal pada IEEE Security and Privacy, 7(6), 22–29.

[4] Cert, & Cert. (2008), *Insider Threat Study*, (June 2005), 0. Tersedia di http://www.dtic.mil/cgi-bin/GetTRDoc?Location=U2&doc=GetTRDoc.pdf&AD=ADA441249

[5] Chinchani, R., Iyer, A., Ngo, H., & Upadhyaya, S. (2005), *A Target-Centric Formal Model For Insider Threat and More*, makalah pada IEEE International Conference, 1–17.

[6] Chinchani, R., Iyer, a., Ngo, H. Q., & Upadhyaya, S. (2005), *Towards a theory of insider threat assessment,* makalah prosiding pada the 2005 International Conference on Dependable Systems and Networks (DSN'05).

[7] Durán, F. A., Conrad, S. H., Conrad, G. N., Duggan, D. P., & Held, E. B. (2009), *Building a system for insider security*, Artikel Jurnal pada IEEE Security and Privacy, 7(6), 30–38.

[8] Eberle, W., Holder, L., & Graves, J. (2011), *Insider Threat Detection Using a Graph-Based Approach*, artikel jurnal pada Journal of Applied Security Research, 6(1), 237–241.

[9] Kammuller, F., & Probst, C. W. (2015), *Modeling and Verification of Insider Threats Using Logical Analysis*, artikel jurnal pada IEEE Systems Journal, PP(99), 1–12.
[10] Magklaras, G. B., & Furnell, S. M. (2005), *A preliminary model of end user sophistication for insider threat prediction in IT systems*, makalah prosiding pada Computers and Security, 24(5), 371–380.
[11] Martinez-Moyano, I. J., Rich, E., Conrad, S., Andersen, D. F., & Stewart, T. R. (2008), *A behavioral theory of insider-threat risks*, artikel jurnal pada ACM Transactions on Modeling and Computer Simulation, 18(2), 1–27.
[12] Nguyen, N., Reiher, P., & Kuenning, G. H. (2003), *Detecting insider threats by monitoring system call activity,* IEEE Systems, Man and Cybernetics Society Information Assurance Workshop, (June), 45–52.
[13] Nurse, J. R. C., Buckley, O., Legg, P. A., Goldsmith, M., Creese, S., Wright, G. R. T., & Whitty, M. (2014), *Understanding Insider Threat: A Framework for Characterising Attacks*, artikel jurnal pada IEEE Security and Privacy Workshops.
[14] Sibai, F. M., & Menascë, D. A. (2011), *Defeating the insider threat via autonomic network capabilities*, makalah pada 3rd International Conference on Communication Systems and Networks, COMSNETS 2011.
[15] Spitzner, L., Technologies, H., & Inc. (2003), *Catching the Insider Threat*, makalah prosiding pada 19th Annual Computer Security Applications Conference, ACSAC 2003.
[16] Wang, Y. L., & Yang, S. C. (2014), *A Method of Evaluation for Insider Threat*, makalah pada International Symposium on Computer, Consumer and Control, 438–441.